

# United States District Court

## EASTERN DISTRICT OF OKLAHOMA

**In the matter of the search of Cellular Phone  
with IMEI Number 353373302378447, Currently  
Located at the Durant Resident Agency, 300  
West Evergreen St, Durant, OK 74701.**

**Case No. 22-MJ-275-JAR**

### APPLICATION FOR SEARCH WARRANT

I, Paul Sparke, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that there is now concealed on the following person or property located in the Eastern District of Oklahoma (*identify the person or describe property to be searched and give its location*):

**SEE ATTACHMENT "A"**

The person or property to be searched, described above, is believed to conceal (*identify the person or describe the property to be seized*):

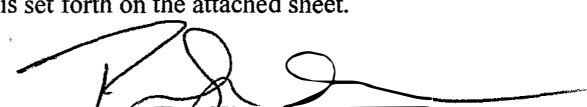
**SEE ATTACHMENT "B"**

The basis for the search under Fed. R. Crim. P. 41(c) is (*check one or more*):

- ☒ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of Title 18, United States Code, Section(s) 2241(c), 2246(2)(A), 1151, and 1152, and the application is based on these facts:

- ☒ Continued on the attached sheet.
- ☐ Delayed notice of \_\_\_\_\_ days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

  
Paul Sparke  
Special Agent  
Federal Bureau of Investigation

Sworn to and signed before me.

Date: October 5, 2022

City and state: Muskogee, Oklahoma

  
\_\_\_\_\_  
Judge's signature  
JASON A. ROBERTSON  
UNITED STATES MAGISTRATE JUDGE  
Printed name and title



**AFFIDAVIT IN SUPPORT OF AN  
APPLICATION UNDER RULE 41 FOR A  
WARRANT TO SEARCH AND SEIZE**

I, Paul Sparke, being first duly sworn, hereby depose and state as follows:

**INTRODUCTION AND AGENT BACKGROUND**

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—an electronic device—which is currently in law enforcement possession and described in **Attachment A**, and the extraction from that property of electronically stored information described in **Attachment B**.

2. I am a Special Agent with the Federal Bureau of Investigation and have been since July 2009. I am currently assigned to the Oklahoma City Division, Durant Resident Agency. In this capacity, I am charged with investigating violations of federal criminal law to include computer intrusions and other crimes involving the use of computers.

3. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

**IDENTIFICATION OF THE DEVICE TO BE EXAMINED**

4. The property to be searched is a cellular phone identified as a CRICKET DREAM 5, IMEI NUMBER 353373302378447, hereinafter the “Device.” The Device is currently located at the FBI Resident Agency in Durant, Oklahoma.

5. The applied-for warrant would authorize the forensic examination of the Device for the purpose of identifying electronically stored data particularly described in **Attachment B**.

### **JURISDICTION**

6. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. §§ 2711 and 3127. As a court of competent jurisdiction, this Court has the authority to order the disclosure of the information sought in **Attachment A**, and the specific probable cause set forth herein. The individual who potentially engaged in criminal activity relevant to the requested search warrant is Dennis Hebert.

### **PROBABLE CAUSE**

7. In July 2021, Dennis Hebert (Hebert) resided at a residence on Buchanan Ave, McAlester, OK 74501 for approximately three days. During this time, security camera recordings show Hebert slept in the same room as a six-year-old minor identified as K.D. Recordings show the defendant masturbating while K.D. was feet away, kissing K.D. on the mouth on multiple occasions, and show the defendant take the camera from the wall while alone in the room with K.D. Further, the security camera recorded Hebert utilizing his cellular phone while K.D. was in the room during the same time period that the above acts were taking place.

8. On July 21, 2021, prior to the indictment, Hebert was interviewed by a Choctaw Nation Tribal Police Officer. After the interview was completed, Hebert used a device believed to be his cellular phone to communicate through Facebook Messenger about the interview and the alleged crime. Within these communications, Hebert stated “the officer guy has already been here he told me that he’s sending his report to the fbi so there’s a good possibility I might go to jail because you were not there to support me when I got accused of this bullshit”. These communications were sent to Government witness K.B. Facebook records provided by K.B. show that in addition to messages relating to this ongoing investigation, Hebert attempted to call her through the application three times following his interview with the Choctaw Nation Tribal Police.

9. On July 26, 2022, Hebert was indicted by a Federal Grand Jury for one count of Aggravated Sexual Abuse in Indian County, 18 USC Section 2241(c), 2246(2)(A), 1151 & 1152.

10. Hebert was arrested on August 31, 2022, while working at a carnival in Erie, PA. At the time of his arrest, Hebert had a cellular phone in his possession (the **Device**). The cellular phone was included in his personal property at the time of his arrest.

11. On September 7, 2022, I obtained a Search Warrant out of the Western District of Pennsylvania to seize the cellular phone. Later the same day, SA Michael Shaffer executed the Search Warrant and seized Hebert's cellular phone.

12. The cellular phone was submitted as evidence and transferred from the Pittsburgh Division to the Oklahoma City Division. The cellular phone is currently in the custody of the FBI in Durant, OK, which is in the Eastern District of Oklahoma.

### **TECHNICAL TERMS**

13. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer

a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic “address books;” sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system (“GPS”) technology for determining the location of the device.

- b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.
- c. Portable media player: A portable media player (or “MP3 Player” or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of

electronic data and may offer additional features such as a calendar, contact list, clock, or games.

- d. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated “GPS”) consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna’s latitude, longitude, and sometimes altitude with a high level of precision.
- e. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving

them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system (“GPS”) technology for determining the location of the device.

- f. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

14. Based on my training, experience, and research, and from consulting the manufacturer’s advertisements and product technical specifications available online at <http://cricketwireless.com>, I know that the Device has capabilities that allow it to serve as a wireless telephone, digital camera, portable media player, GPS navigation device, PDA, and can access the internet. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

#### **ELECTRONIC STORAGE AND FORENSIC ANALYSIS**

15. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

16. *Forensic evidence.* As further described in **Attachment B**, this application seeks permission to locate not only electronically stored information that might serve as direct evidence

of the crimes described on the warrant, but also forensic evidence that establishes how the Device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Device because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).
- b. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.
- c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.



- e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

17. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

18. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

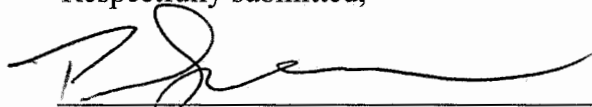
### CONCLUSION

19. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the Device described in **Attachment A** to seek the items described in **Attachment B**.

20. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711(3) and 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that - has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(I).

21. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

Respectfully submitted,

A handwritten signature in black ink, appearing to read 'Paul Sparke', written over a horizontal line.

Paul Sparke  
Special Agent  
Federal Bureau of Investigation

Subscribed and sworn to before me  
on October 5, 2022:

A handwritten signature in blue ink, appearing to read 'Jason A. Roberts', written over a horizontal line.

UNITED STATES MAGISTRATE JUDGE

**ATTACHMENT A**

The property to be searched is a cellular phone identified as a CRICKET DREAM 5, IMEI NUMBER 353373302378447, hereinafter the "Device." The Device is currently located at the FBI Resident Agency in Durant, Oklahoma.

This warrant authorizes the forensic examination of the Device for the purpose of identifying the electronically stored information described in **Attachment B**.

**ATTACHMENT B**

**Particular Things to be Seized and Procedures  
to Facilitate Execution of the Warrant**

All records on the **Device** described in **Attachment A** that relate to violations of 18 U.S.C. § 2241(c) involving **DENNIS HEBERT** and other co-conspirators, including, but not limited to:

1. dialed outgoing telephone/pager numbers;
2. incoming telephone/pager numbers;
3. missed incoming telephone/pager numbers;
4. numeric/alphanumeric messages sent or received;
5. verbal messages sent or received;
6. address and telephone/pager number listings;
7. electronically composed memorandum;
8. time and or data markings to include calendar format organization of all such data;
9. phone book listings to include names, aliases, telephone/pager numbers, codes, types of phone numbers and addresses;
10. photos and videos;
11. historical GPS locations;
12. internet web browser history data;
13. records of Internet Protocol addresses used; and
14. records of Internet activity, including firewall logs, caches, browser history and cookies, “bookmarked” or “favorite” web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

15. child pornography, as defined in 18 U.S.C. § 2256(8), visual depictions of minors engaging in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2), and child erotica.

As used above, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.